International Journal of Computer Science Engineering & Technology
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)– NEW DELHI INDIA .
ISSN :2455-9091

ENABLING CLOUD STORAGE AUDITING WITH VERIFIABLE OUTSOURCING OF KEY UPDATES

[1] N. Vignesh M.E., [2] T. Sivakumar M.E.,
[1] Maharaja Institute of Technology Coimbatore.
[2] HOD of CSE Dept, Maharaja Institute of Technology Coimbatore.

ABSTRACT: It greatly attracts attention and interest from both academia and industry due to the profitability, but it also have challenges that must be handled before coming to our real life to the best of our knowledge. Data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. Secondly, personal information (defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers. We present an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption by using OPE (Order Preserving Encryption) Algorithm. The new approach is simple, general, and almost optimal. A fix for that problem could involve compression of the encrypted data, but this would put a large amount of strain on the backend and undeniably cause slower speeds of service, another big concern for internet companies.

Keywords: [Cloud Computing, Data Privacy, OPE Algorithm]

1. INTRODUCTION

In recent years, cloud storage service has become a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients' data. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud (or hybrid cloud). Often, by using virtual infrastructure management (VIM), a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2.The people whose concern is the cloud security continue to hesitate to transfer their business to cloud. Security issues have been the dominate barrier of the development and widespread use of cloud computing.

Outsourcing brings down both capital expenditure (CapEx) and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive/classified data is out of the owners' control.

The scope of the project is Attribute-based Encryption have been proposed to secure the cloud storage. We present a semi anonymous privilege control scheme anonymity control to address not only the data privacy, but also the user identity privacy in existing access Control schemes. User revocation is a great challenge in the application of ABE schemes.

This paper is organized as follows: in section II, we discuss about related works and the characteristics of Cloud privacy issues, section III discuss about the problem definition of previous works, section IV focuses on proposed system implementations, section V discuses about the methodology, section VI concludes the work.

2. RELATED WORKS

It can express arbitrarily general encryption policy our system also tolerates the compromise attack towards attributes Authorities, which is not covered in many existing works. Those schemes introduce accountability such that malicious users' keys can be traced. On the other hand, similar direction as ours can be found, who try to hide encryption policy in the cipher texts, but their solutions do not prevent the attribute disclosure in the key generation phase.

Attribute Based Encryption with Privacy Preserving using Asymmetric Key in Cloud Computing [1] Symmetric key algorithm uses same key for both encryption and decryption. The authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. A new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. The validity of the user who stores the data is also verified. On multi-authority cipher text-policy attribute-based encryption [2] In classical encryption schemes, data is encrypted under a single key that is associated with a user or group. In Cipher text-Policy Attribute-Based Encryption (CP-ABE) keys are associated with attributes of users, given to them by a central trusted authority, and data is encrypted under a logical formula over these attributes. Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services [3] Cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and productivity enhancements by using cloud-based services to manage projects, to make collaborations. Secure Data Retrieval Based on Cipher text Policy Attribute-Based Encryption (CP-ABE) System for the DTNs [4] Disruption Tolerant Network (DTN) technologies are designed to enable nodes in such environments to communicate with one another. Several application scenarios require a security design that provides fine grain access control to contents stored in storage nodes within a DTN or to contents of the messages routed through the network. Security Architecture for Data Aggregation and Access Control in Smart Grids [5] Data can be aggregated by home area network, building area network and neighboring area network in such a way that the privacy of customers is protected. We use holomorphic encryption technique to achieve this. The

consumer data that is collected is sent to the substations where it is monitored by remote terminal units (RTU). The proposed access control mechanism gives selective access to consumer data stored in data repositories and used by different smart grid users. Users can be maintenance units, utility centers, pricing estimator units or analyzing and prediction groups. We solve this problem of access control using cryptographic technique of attribute-based encryption.

3. PROBLEM DEFINITION

A user can decrypt the cipher text if and only if the access tree in his private key is satisfied by the attributes in the cipher text. However, the encryption policy is described in the keys, so the encrypted does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation. A user may be entitled some new attributes or revoked some current attributes. And his permission of data access should be changed accordingly. However, existing attribute revocation methods either rely on a trusted server or lack of efficiency, they are not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.

4. PROPOSED SYSTEM

The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F. We firstly implement the real toolkit of a multi authority based encryption scheme AnonyControl and AnonyControl-F.

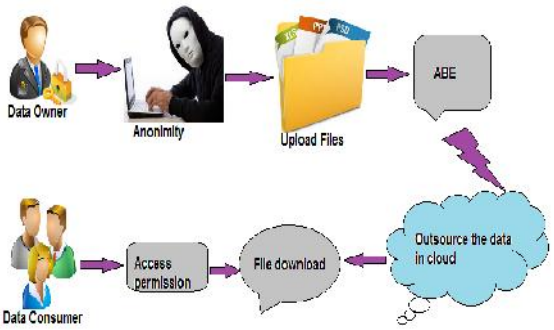

Figure 1: Control cloud access data permission and anonymity with fully attribute based encryption

4.1 User Interface Design

The main idea of this module is to design the user interface for users in the project. The login page is to design for data owner and data user. After the data owner logins into the system, the page displayed which allows the data owner to achieve the encrypted file upload to the system. When the user logins to the system, the system allows the user to input the decryption key and attributes for retrieval of specified file.

4.2 File Encryption

Each file which is to be uploaded is encrypted with encryption key. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Owner specifies the set of attributes for access structure, it then encrypts the file. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system.

4.3 Key Generation and Distribution

While data owner uploading the encrypted file, they also upload set of attributes. The data owner gives the attributes of the receiver while sending the file to the receiver; the file gets encrypted as per the given attributes. Thus the attributes for specified file is to be distributed and decryption key for decrypting the file are to be distributed to the data users.

4.4 File Access

User requests the file by providing attributes and in response system replies with encrypted file. Before that the system will check the

attributes of the users whether the receiver have the same attributes as the sender mentioned.

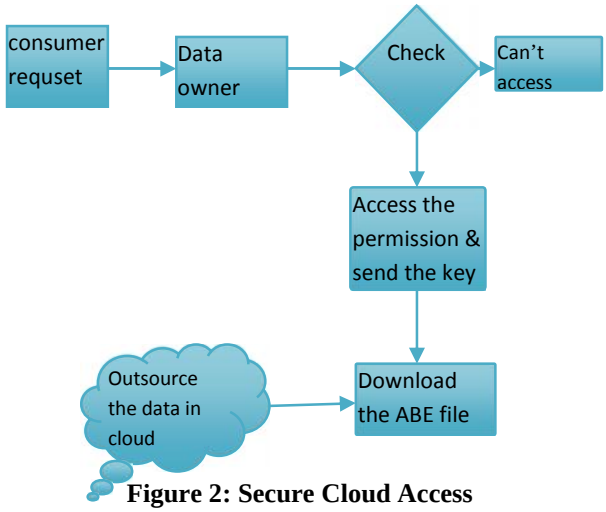

Figure 2: Secure Cloud Access

It will avoid the unauthorized users or hackers. The receiver receives the encrypted file, and he has given the attributes, if it's correct, the original file gets decrypted for the receiver. This allows them to access information without authorization and thus poses a risk to information privacy.

5. METHODOLOGY

Order preserving encryption (OPE) is a very important technique for database related applications due to its capability of supporting range query processing directly 1 on encrypted data without needing to decrypt them and expose them to potential attackers who may have compromised the system. The OPEs do not have perfect security since the ciphertexts leak the ordering information of the plaintexts. But on the other hand, when it is desirable to have a reasonable performance for range query processing while achieving a reasonable degree of security protection, the OPE scheme can be used as long as there is a good understanding of its security risks. However, how secure is the OPE scheme has not been sufficiently analyzed and further research is needed to investigate its security properties. There are various constructions of the OPE scheme. In the proposed OPE algorithm first generates a sequence of random numbers and then encrypts an integer x to the sum of the first x random numbers. In a sequence of strictly increasing polynomial functions are used to construct the OPE algorithm. The encryption of an integer x is the outcome of the iterative operations of those functions on x. The OPE algorithm is constructed by using a mapping function composed of partition and identification functions. The partition function divides the range into multiple partitions, and the identification function assigns an identifier to each partition.

OPE algorithm following three steps: modeling the input and target distributions, flattening the plaintext database into a flat database, and transforming the flat database into the cipher database. However, security analysis for these and other OPE algorithms has been fully investigated.

CONCLUSION

We have proposed a single keyword search scheme to make encrypted data search efficient. However, there are still some possible extensions of our current work remaining. We would like to propose a multi-keyword search scheme to perform encrypted data search over mobile cloud in future. As our OPE algorithm is a simple one, another extension is to find a powerful algorithm which will not harm the efficiency.

REFERENCE

[1]. L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2]. X. Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[3]. D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[4]. O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition

intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.
[5]. J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.
[6]. J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.
[7]. A. A. Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing documents and images. Morgan Kaufmann Pub, 1999.
[8]. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.